

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of:	§	Filed: April 8, 2004
Garbow et al.	§	
	§	Group Art Unit: 2134
Serial No.: 10/821,159	§	
	§	Examiner: Yonas A. Bayou
Confirmation No.: 9191	§	

For: METHOD AND APPARATUS FOR GOVERNING THE TRANSFER OF
PHYSIOLOGICAL AND EMOTIONAL USER DATA

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office to fax number 571-273-8300 to the attention of Examiner Yonas A. Bayou, or electronically transmitted via EFS-Web, on the date shown below:

October 14, 2008	/Joseph Jong/
Date	Joseph Jong

Dear Sir:

APPEAL BRIEF

Applicants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2134 dated May 22, 2008, finally rejecting claims 1-10. The final rejection of claims 1-10 is appealed. This Appeal Brief is believed to be timely since it is transmitted by the due date of October 14, 2008, as set by the filing of a Notice of Appeal on August 14, 2008.

Please charge the fee of \$540.00 for filing this brief to:

Deposit Account No. 09-0465 / ROC920030400US1.

TABLE OF CONTENTS

1.	Identification Page.....	1
2.	Table of Contents	2
3.	Real Party in Interest	3
4.	Related Appeals and Interferences	4
5.	Status of Claims	5
6.	Status of Amendments	6
7.	Summary of Claimed Subject Matter	7
8.	Grounds of Rejection to be Reviewed on Appeal	8
9.	Arguments	9
10.	Conclusion	13
11.	Claims Appendix	14
12.	Evidence Appendix	16
13.	Related Proceedings Appendix	17

Real Party in Interest

The present application has been assigned to International Business Machines Corporation, Armonk, New York.

Related Appeals and Interferences

Applicant asserts that no other appeals or interferences are known to the Applicant, the Applicant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-10 are pending in the application. Claims 1-34 were originally presented in the application. Claims 11-34 have been canceled without prejudice. Claims 1-10 stand finally rejected as discussed below. The final rejections of claims 1-10 are appealed. The pending claims are shown in the attached Claims Appendix.

Status of Amendments

All claim amendments have been entered by the Examiner, including amendments to the claims proposed after the final rejection.

Summary of Claimed Subject Matter

Claimed embodiments include methods (see claims 1-10) for governing the secure transfer of data characterizing a user's behavior, physiological parameters and/or psychological parameters.

CLAIM 1 – INDEPENDENT

Claim 1 recites a method comprising receiving, from a requesting application, a request for emotion data characterizing an emotional state of a user, wherein the requesting application is of a particular type (See Application, P. 0006:1-2, Fig. 4:412). The method further comprises accessing a firewall ruleset defining rules governing the transfer of the emotion data to requesting applications, wherein at least some of the rules of the firewall ruleset each specify a different application type selected from a plurality of application types (See P. 0006:2-4, P. 0029:1-2, P. 0032: 1-5, and Fig. 4: 414). The method also comprises determining whether to provide the emotion data to the requesting application (See P. 0006: 4-5, Fig. 4: 416). Wherein the determining comprises locating each rule in the firewall ruleset that includes a parameter specifying the particular type of the requesting application (See P. 0044: 14-15, P. 0032: 1-3, P. 0039: TABLE: Illustrative Ruleset Parameters: Entries 1 and 2), determining whether the located rules are satisfied (See: P. 0044: 15-17, Fig. 4: 416); whereby the rules are applied to each requesting application according to its respective application type (See P. 0032: 1-3), and denying the request if the firewall ruleset rules are not satisfied (See P. 0006: 5-6, Fig. 4: 418).

Grounds of Rejection to be Reviewed on Appeal

1. Rejection of claims 1-10 under 35 U.S.C. § 102(e) as being anticipated by *Abbott et al.*, U.S. Pat. No. 7,046,263 (hereinafter *Abbott*).

ARGUMENTS

1. Rejection of claims 1-10 under 35 U.S.C. § 102(e) as being anticipated by *Abbott*.

The Applicable Law

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). As demonstrated below, *Abbott* does not disclose "each and every element as set forth in the claim."

The Reference

Abbott provides for a software facility to exchange information between sensors and applications in a wearable computer system. See *Abbott* Col. 2: 55-57. A Characterization Module (CM) receives attribute values from a Context Server (CS), each value being either directly measured by a sensor, or derived from other measured values. See Col. 4: 39-43, 57-59. The CM then caches the data for use when responding to requests from a Context Client (CC) for the value of a given attribute. See Col. 4: 59-60.

The criteria used by the CM when responding to a request from a CC are whether a value for the requested attribute has been cached and, if so, whether that value is sufficiently accurate and/or recent. See Col. 4: 60-66. In addition to these criteria for supplying data, *Abbot* discloses a security check using either password

protection or digital signing technology. See Col. 17: 51-58, Fig. 19:1915, Fig. 20A: 2012. Finally, *Abbott* discloses that, in one exemplary context, an attribute could contain information regarding the user's desired output behavior for other information. See Col. 8: 61-62. This desired output behavior could limit the output of private family information only to members of that family. See Col. 8: 62-64.

Argument

Abbott does not disclose a number of features found in claims 1-10. For example, *Abbott* does not disclose "wherein at least some of the rules of the firewall ruleset each specify a different application type selected from a plurality of application types." Further, *Abbott* does not disclose "locating each rule in the firewall ruleset that includes a parameter specifying the particular type of the requesting application; and determining whether the located rules are satisfied; whereby the rules are applied to each requesting application according to its respective application type."

The Examiner's Argument

The Examiner has argued that the above features are disclosed by *Abbott* at 5:25-29; 15:51-57, 16:65 – 17:3; 19:2-6; 24:10-23 fig. 20A and fig. 23. However, the cited passages and figures are silent to both application type and firewall rulesets, as found in the plain language of the claim. Throughout prosecution the Examiner has not addressed *Abbott's* silence regarding application type. Regarding the firewall ruleset, the Examiner takes the position that the security authorization found in *Abbott* in Fig. 20A corresponds to a firewall.

The Examiner further alleges that *Abbott* discloses attribute values that can have "a variety of types of information related to [them]," and that this related information "can be used... to determine whether and how to supply the values."

Applicants' Response to the Examiner's Argument

First, as described above, there is very little restriction of the flow of data disclosed in *Abbott*. Specifically, data is freely transferred to a requesting entity in *Abbott* except in two distinct instances. First, there is the security authorization which can be found in Figures 19 and 20A and is described in Column 17, lines 51 -58 as a security check using either password protection or digital signing technology. Second, there is the case where an attribute value itself contains user based information on the sensitivity of given data. See Col. 8: 61-64.

Abbott is silent as to whether these two forms of restricting data can or should be taken together. However, even assuming that both forms could be taken together, *Abbott* would still fail to disclose a “firewall ruleset” much less a “firewall ruleset that includes a parameter specifying the particular type of the requesting application” as claimed. At most, *Abbott* could disclose a security authorization scheme based not on application type but based only on the identity of the requestor. To reiterate, the only examples of securing data found in *Abbott* are using a password (Col. 17: 57), digital signing (Col. 17: 57-58), and restricting access to members of a family (Col. 8: 63-64). Each of these examples is a form of security based on the identity of the requestor, not an application type.

Second, regarding information related to attribute values determining whether and how to supply those values, Applicants fail to see how this reads upon the claim language. While *Abbott* does teach associating different types of information with a given attribute value, these associations are not used as part of the security authorization, except insofar as the recited example of sensitive family data. In fact, Figure 23 of *Abbott*, which shows such an association, is completely silent as to security authorization. Again, as stated above, security authorization in *Abbott* is based upon the identity of the requestor, and not upon any other “type of information” associated with a given value, much less the specific “type of information” claimed. That is, the security authorization is not based upon the particular application type requesting the value. In this regard, the Examiner cites to *Abbott*'s table of possible types of

information that can be related to a value. See Col. 24: 26-39. However, “application type” is not found in this table.

Therefore, *Abbott* does not disclose the claimed features of “wherein at least some of the rules of the firewall ruleset each specify a different application type selected from a plurality of application types;” and “locating each rule in the firewall ruleset that includes a parameter specifying the particular type of the requesting application; and determining whether the located rules are satisfied; whereby the rules are applied to each requesting application according to its respective application type.”

CONCLUSION

The Examiner errs in finding that claims 1-10 are anticipated by *Abbott*.

Withdrawal of the rejections and allowance of all claims is respectfully requested.

Respectfully submitted, and
S-signed pursuant to 37 CFR 1.4,

/Gero G. McClellan, Reg. No. 44,227/

Gero G. McClellan
Registration No. 44,227
Patterson & Sheridan, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846
Attorney for Appellant(s)

CLAIMS APPENDIX

1. (Previously Presented) A method comprising:
 - receiving, from a requesting application, a request for emotion data characterizing an emotional state of a user, wherein the requesting application is of a particular type;
 - accessing a firewall ruleset defining rules governing the transfer of the emotion data to requesting applications, wherein at least some of the rules of the firewall ruleset each specify a different application type selected from a plurality of application types;
 - determining whether to provide the emotion data to the requesting application; wherein determining comprises:
 - locating each rule in the firewall ruleset that includes a parameter specifying the particular type of the requesting application; and
 - determining whether the located rules are satisfied; whereby the rules are applied to each requesting application according to its respective application type; and
 - denying the request if the firewall ruleset rules are not satisfied.
2. (Original) The method of claim 1, providing the requested emotion data to the requesting application if the firewall ruleset rules are satisfied.
3. (Original) The method of claim 1, providing only a portion of the requested emotion data to the requesting application if the firewall ruleset rules are satisfied.
4. (Original) The method of claim 1, wherein the emotional state characterized by the emotion data is one of angry, sad, happy, excited, nervous, interested and any combination thereof.
5. (Original) The method of claim 1, wherein the emotional state characterized by the emotion data is any calculable human emotion.

6. (Original) The method of claim 1, wherein the firewall ruleset is configurable by the user.
7. (Original) The method of claim 1, wherein the requesting application is a web-based application and the request is received via the Internet.
8. (Original) The method of claim 1, wherein the emotion data is based on measurements of physiological parameters.
9. (Original) The method of claim 8, wherein the measurements of physiological parameters, comprise at least one of blood pressure, pulse and galvanic skin response.
10. (Original) The method of claim 8, wherein the measurements of physiological parameters, comprise measurements of brain wave activity of the user.
- 11 – 34. (Cancelled)

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.